Claims

Having thus described our invention, what we claim as new, and desire to secure by Letters Patent is:

1. A method for securely providing data of a content provider to a user without trusting an internet service provider, said method comprising:
   a. generating a first key known only to said content provider;
   b. encrypting a second key using said first key and an encryption algorithm requiring a one-time password;
   c. storing said encrypted second key on a client machine; and
   when said user desires to access said data:
   d. decrypting said second encrypted key using said first key; and
   e. accessing said data using said second key.

2. A method as recited in claim 1, further comprising the step of transmitting the identity of said client machine to said content provider to authenticate that said user is using said client machine, thereby permitting said data to be accessed only on said client machine.

3. A method as recited in claim 1, wherein said one-time password is a unique user identifier and wherein said one-time password is transmitted out of band.

4. A method as recited in claim 1, wherein said second key is required in an algorithm that generates a session key which is used to decrypt said data.

5. A method for securely providing data of a content provider to a user without trusting an internet service provider, said method comprising:
   a. generating a first key known only to said content provider;
   b. encrypting a second key using said first key and an encryption algorithm requiring a one-time password and a separate user provided password;
   c. storing said encrypted second key on a client machine; and
   when said user desires to access said data:
   d. decrypting said second encrypted key using said user provided password; and

e. accessing said data using said second key.

6. A method as recited in claim 5, further comprising the step of transmitting the identity of said client machine to said content provider to authenticate that said user is using said client machine, thereby permitting said data to be accessed only on said client machine.

7. A method as recited in claim 5, wherein said one-time password is a unique user identifier and wherein said one-time password is transmitted out of band.

8. A method as recited in claim 5, wherein said second key is required in an algorithm that generates a session key which is used to decrypt said data.

9. In a communications network having at least a content provider node and a plurality of client machines, a method of authenticating a user seeking access to secure data of said content provider, said method comprising:

a. transmitting g^a and the identity of the user of said one client machine to said content provider node, where g and a are random numbers and where a is known only to said client machine, and where g is known to both content provider node and said client machine;
b. generating g^b , where b is known only to said content provider node;
c. encrypting g^b with a one-time password of said user;
d. calculating g^(a*b) by said client machine using said one-time password to decrypt said encrypted g^b; and
e. transmitting g^(a*b) to said content provider, whereby said client machine's knowledge of g^(a*b) authenticates said user to said content provider.

10. A method as recited in claim 9, further comprising the step of transmitting the identity of a particular one of said client machines to said content provider to authenticate that said user is using said client machine, thereby permitting said data to be accessed only by said user on said client machine.

11. A method as recited in claim 9, further comprising the step of performing a method authenticated code on g^(a*b) at said content provider and transmitting results of performing said method authenticated code to said
client, where said client machine verifies said results to authenticate said content provider.

12. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for securely providing data of a content provider to a user, said method comprising:

a. generating a first key known only to said content provider;

b. encrypting a second key using said first key and an encryption algorithm requiring a one-time password;

c. storing said encrypted second key on a client machine; and

when said user desires to access said data:

d. decrypting said second encrypted key using said first key; and

e. accessing said data using said second key.

13 . A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for securely providing data of a content provider to a user, said method comprising:

a. generating a first key known only to said content provider;

b. encrypting a second key using said first key and an encryption algorithm requiring a one-time password and a separate user provided password;

c. storing said encrypted second key on a client machine;

when said user desires to access said data:

d. decrypting said second encrypted key using said user provided password; and

e. accessing said data using said second key.

14. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for use in a communications network having at least a content provider node and a plurality of client machines, said method steps authenticating a user seeking access to secure data of said content provider, said method steps comprising:

a. transmitting g^a and the identity of the user of said one client machine to said content provider node, where g and a are random numbers and where a is known only to said client machine, and where g is known to both content provider node and said client machine;

b. generating g^b , where b is known only to said content provider node;

c. encrypting g^b with a one-time password of said user;
d. calculating g^(a*b) by said client machine using said one-time password to decrypt said encrypted g^b; and
e. transmitting g^(a*b) to said content provider, whereby said client machine's knowledge of g^(a*b) authenticates said user to said content provider.

15. A computer program product for securely providing data of a content provider to a user without trusting an internet service provider, said computer program product comprising:
a. first instruction means for generating a first key known only to said content provider;
b. second instruction means for encrypting a second key using said first key and an encryption algorithm requiring a one-time password;
c. third instruction means for storing said encrypted second key on a client machine; and when said user desires to access said data;
d. fourth instruction means for decrypting said second encrypted key using said first key; and
e. accessing said data using said second key.

16 . A computer program product for securely providing data of a content provider to a user without trusting an internet service provider, said computer program product comprising:
a. first instruction means for generating a first key known only to said content provider;
b. second instruction means for encrypting a second key using said first key and an encryption algorithm requiring a one-time password and a separate user provided password;
c. third instruction means for storing said encrypted second key on a client machine; and when said user desires to access said data;
d. fourth instruction means for decrypting said second encrypted key using said user provided password; and
e. fifth instruction means for accessing said data using said second key.

17. A computer program product for use in a communications network having at least a content provider node and a plurality of client machines, said computer program for authenticating a user seeking access to secure data of said content provider, said computer program product comprising:

a. transmitting g^a and the identity of the user of said one client machine to said content provider node, where g and a are random numbers and where a is known only to said client machine, and where g is known to both content provider node and said client machine;

b. generating g^b , where b is known only to said content provider node;

c. encrypting g^b with a one-time password of said user;

d. calculating g^(a*b) by said client machine using said one-time password to decrypt said encrypted g^b; and

e. transmitting g^(a*b) to said content provider, whereby said client machine's knowledge of g^(a*b) authenticates said user to said content provider.